Collaboration and security in CNL's virtual laboratory

Andrew Tokmakoff[1], Yuri Demchenko[2] and

Martin Snijders[1]

WACE 2004, Nice, Fr.

[1]Telematica Instituut, [2]Universiteit van Amsterdam

Telematica
Instituut

The CNL Virtual Laboratory

- Our focus is to demonstrate a Virtual Laboratory that could be commercially operable.
  - Consortium of partners includes:

Corus, FEI, DSM, Philips, The University of Amsterdam and The Telematica Instituut.

- Moving from Academic Collaboratories towards Industry-based:
  - Business and Security aspects require more attention

Virtual Lab Usage Scenarios

	Scenario 1: Virtual Laboratory Unlimited	**Scenario 2: Customer watching over the analyst's shoulder**	**Scenario 3: Outsourcing and collaboration**
Summary	Instruments are remotely accessed and controlled. Analysts collaborate remotely and with external experts.	Instruments are locally operated. Customers watch during the analysis and discuss results with the analyst.	Parts of the analysis are outsourced, including operation of instruments. The inquiring and the executing analyst collaborate on analysis of the results achieved.
Lab instruments	Outsourced	In-house	Outsourced
Analysis knowledge	In-house with external consultation	In-house knowledge and customers' knowledge is shared	In-house with external consultation
Measurement knowledge	In-house with external consultation	In-house	Outsourced

- Is a function of "who owns the instruments" and "who provides the analysis/operator expertise"

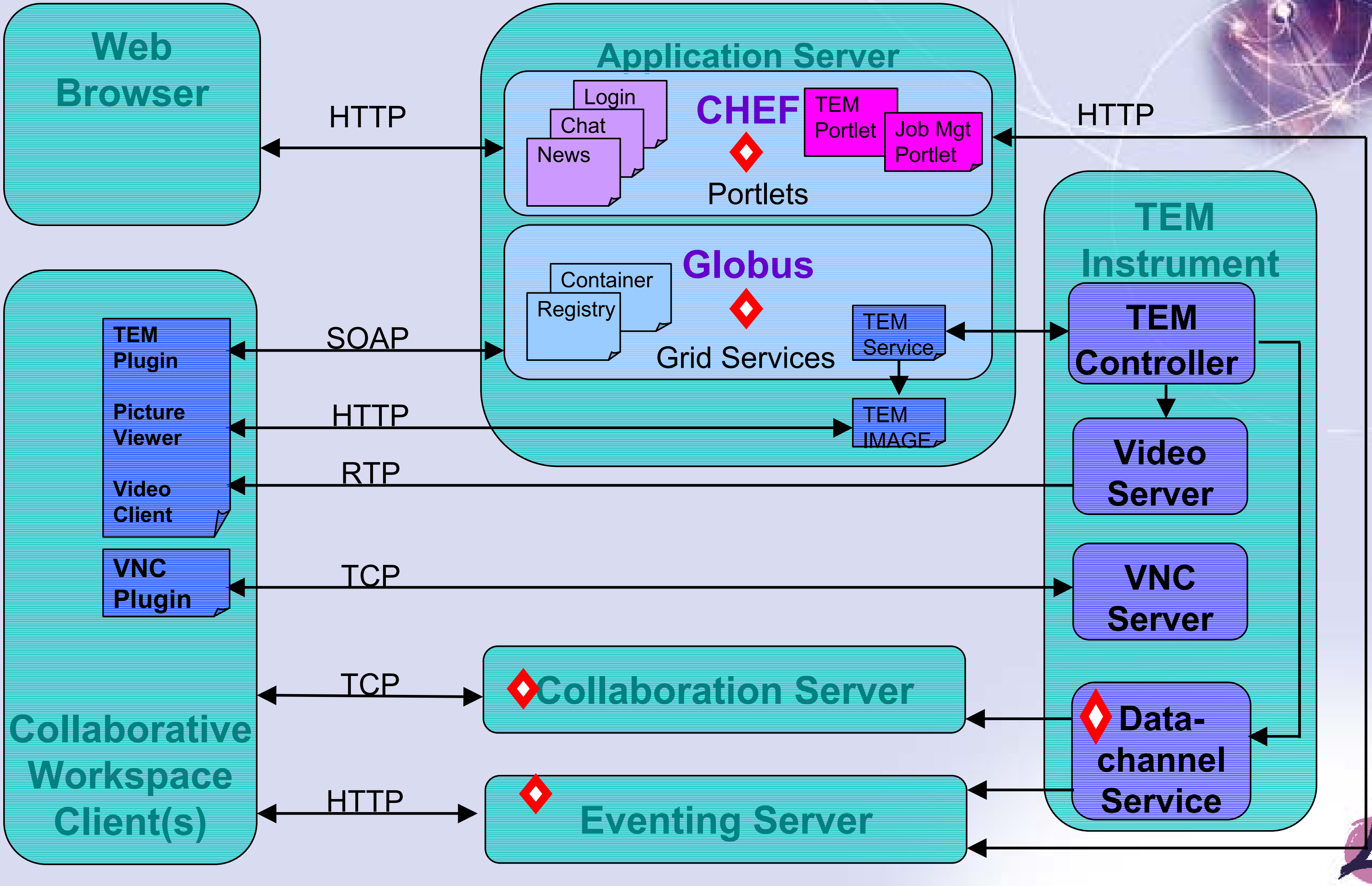
Key Functional Requirements

- Collaborative Remote access and control of Lab Instruments
  - Flexible to allow new Instruments and Control apps to be added.
- Security
  - Job data Integrity, Confidentiality (commercially sensitive data).
  - Restrict instrument access to authorised users at the “scheduled” times.
- Business Enablers
  - Metering and Charging
  - Sample Tracking and Tracing
  - Resource Scheduling
- Interoperability with emerging Scientific Computation Infrastructure standards (OGSA - Grid)

Job-centric Approach

- Jobs are a “key concept”
  - Basic unit of transaction – everything revolves around them
  - Contains:
    - Job processing information (workflow),
    - details regarding the sample(s) to be analysed,
    - the customer who commissioned the work,
    - the instruments (denoted as Resources) used within the Job,
    - the users (and their Role) in the Job.
- Security on Jobs
  - Authorisation of Actions based upon Role and Job Context (RBAC)
- Collaboration – workspaces are based upon Jobs

System Architecture



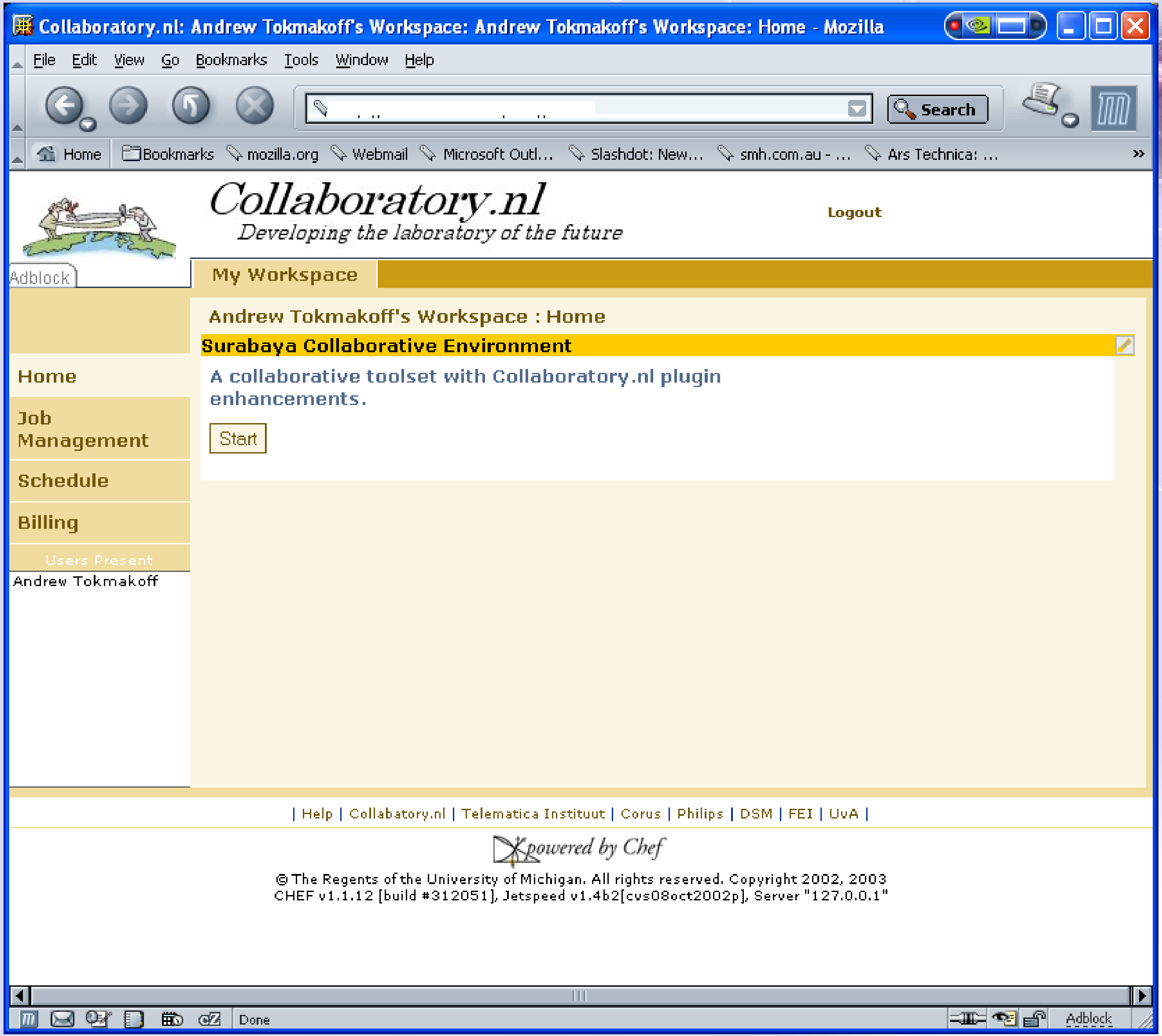
WACE, September 23, 2004

Telematica Instituut

Software Development Approach

- Evolutionary Delivery
  - Start with an initial system concept.
  - Subsequent Requirements and System Design.
  - Iterate: Develop a version, deliver it, obtain and act on feedback.
  - Deliver final version.
- Design-to-Tools Philosophy
  - Build in features that have clear Component (e.g. libraries/application platforms) support
- Leverage Existing tools/components
  - Tomcat/Apache, Chef, Globus, JMF, VNC, Surabaya, Syncshare

Virtual Laboratory Portal



Collaboratory.nl

Developing the laboratory of the future

Andrew Tokmakoff's Workspace : Home

Surabaya Collaborative Environment

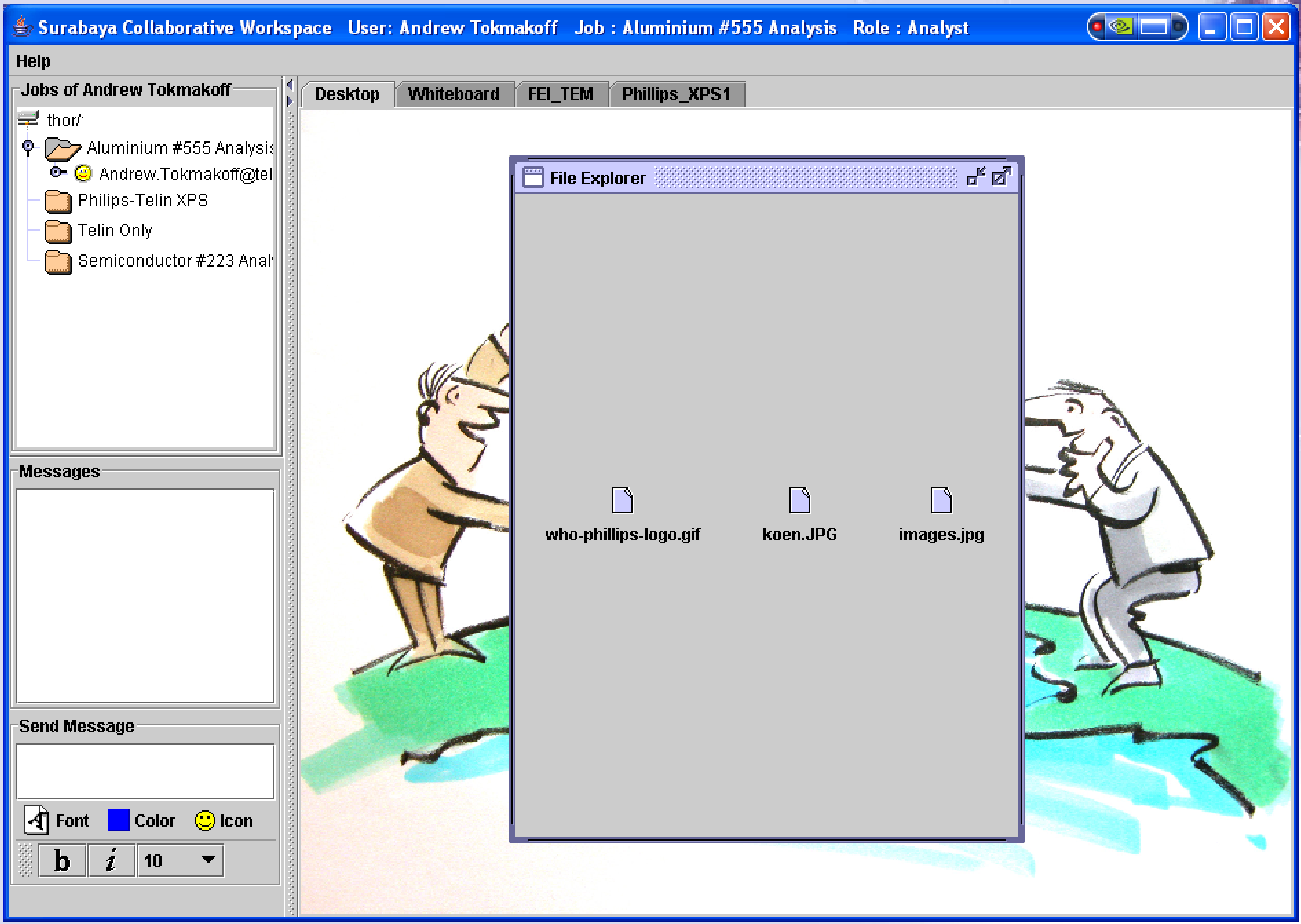
A collaborative toolset with Collaboratory.nl plugin enhancements.

| Help | Collabatory.nl | Telematica Instituut | Corus | Philips | DSM | FEI | UvA |

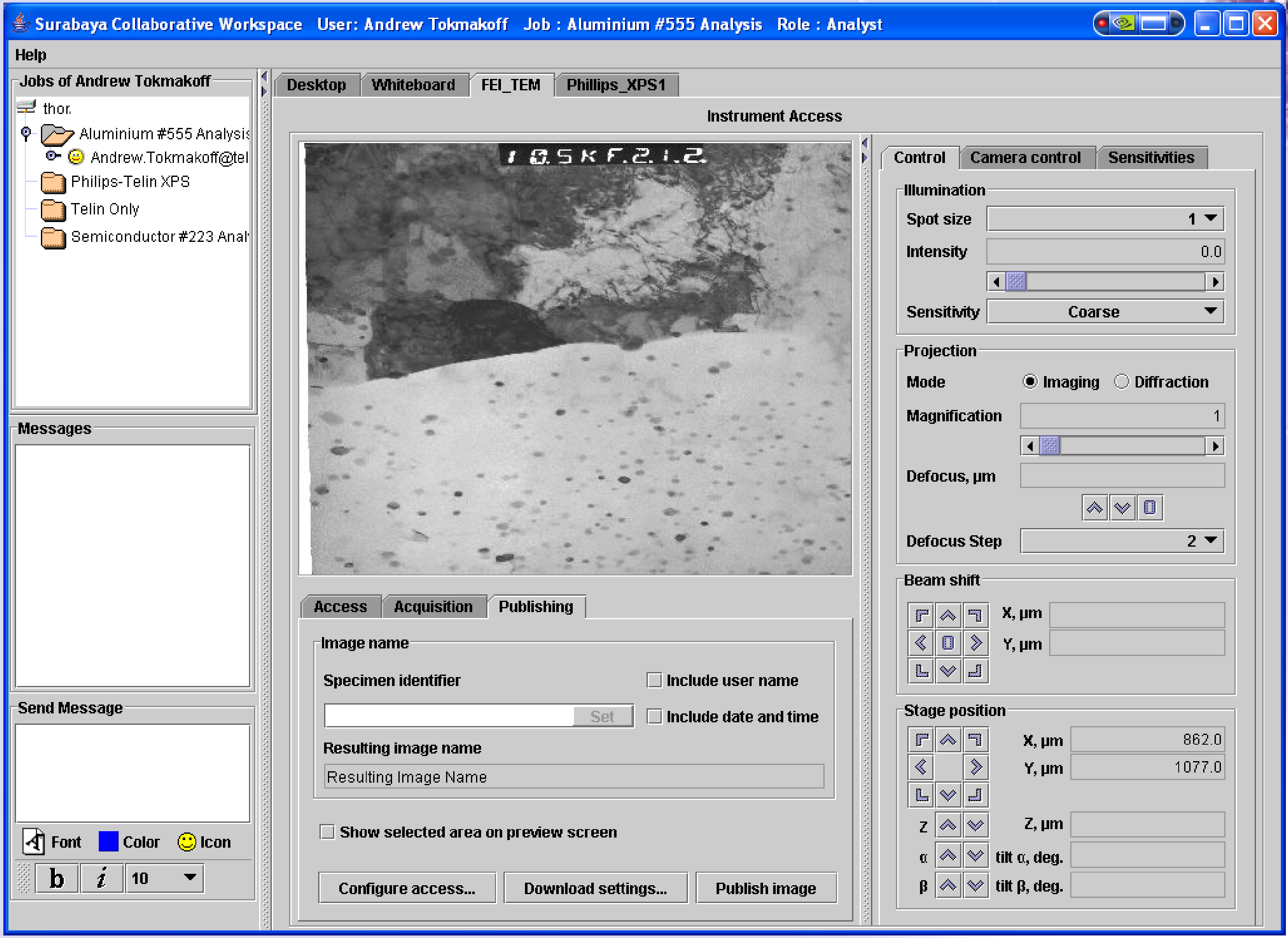
powered by Chef

© The Regents of the University of Michigan. All rights reserved. Copyright 2002, 2003
CHEF v1.1.12 [build #312051], Jetspeed v1.4b2[cvs08oct2002p], Server "127.0.0.1"

Collaborative Tooling



TEM Instrument Tool



Surabaya Collaborative Workspace User: Andrew Tokmakoff Job : Aluminium #555 Analysis Role : Analyst

Help

Jobs of Andrew Tokmakoff
- thor.
  - Aluminium #555 Analysis
    - Andrew.Tokmakoff@tel
  - Philips-Telin XPS
  - Telin Only
  - Semiconductor #223 Anal

Messages

Send Message

Font Color Icon

b *i* 10

Desktop | Whiteboard | FEI_TEM | Phillips_XPS1

Instrument Access

Access | Acquisition | Publishing

Image name

Specimen identifier

□ Include user name

Set

□ Include date and time

Resulting image name: Resulting Image Name

□ Show selected area on preview screen

Configure access... | Download settings... | Publish image

Control | Camera control | Sensitivities

Illumination

Spot size	1
Intensity	0.0
Sensitivity	Coarse

Projection

Mode: ● Imaging ○ Diffraction

Magnification	1
Defocus, µm	
Defocus Step	2

Beam shift

X, µm

Y, µm

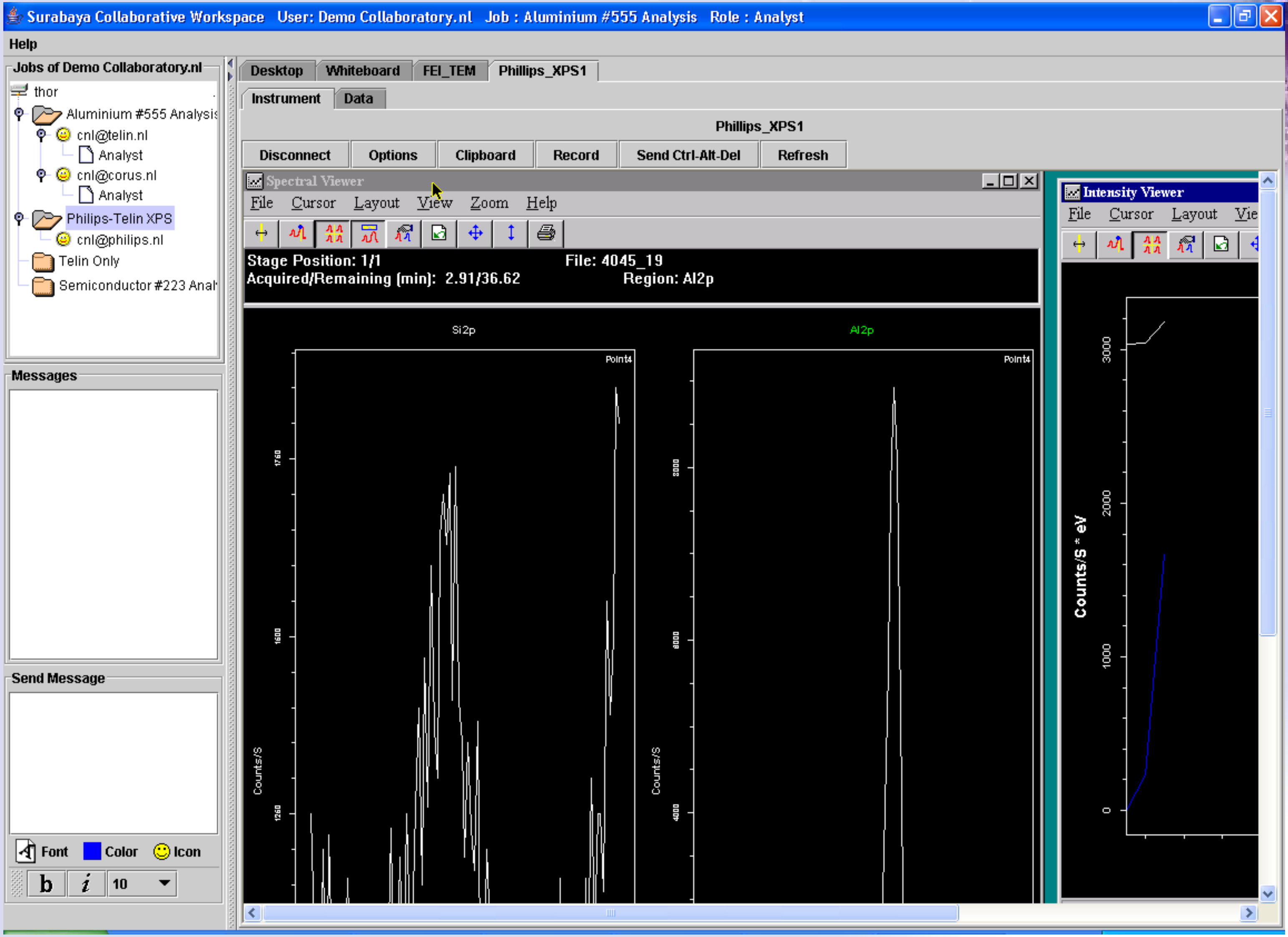
Stage position

X, µm	862.0
Y, µm	1077.0
Z, µm	
tilt α, deg.	
tilt β, deg.	

WACE, September 23, 2004

Telematica Instituut

Remote Desktop - XPS



Surabaya Collaborative Workspace User: Demo Collaboratory.nl Job : Aluminium #555 Analysis Role : Analyst

Jobs of Demo Collaboratory.nl

- thor
  - Aluminium #555 Analysis
    - cnl@telin.nl
      - Analyst
    - cnl@corus.nl
      - Analyst
  - Philips-Telin XPS
    - cnl@philips.nl
  - Telin Only
  - Semiconductor #223 Anal

Phillips_XPS1

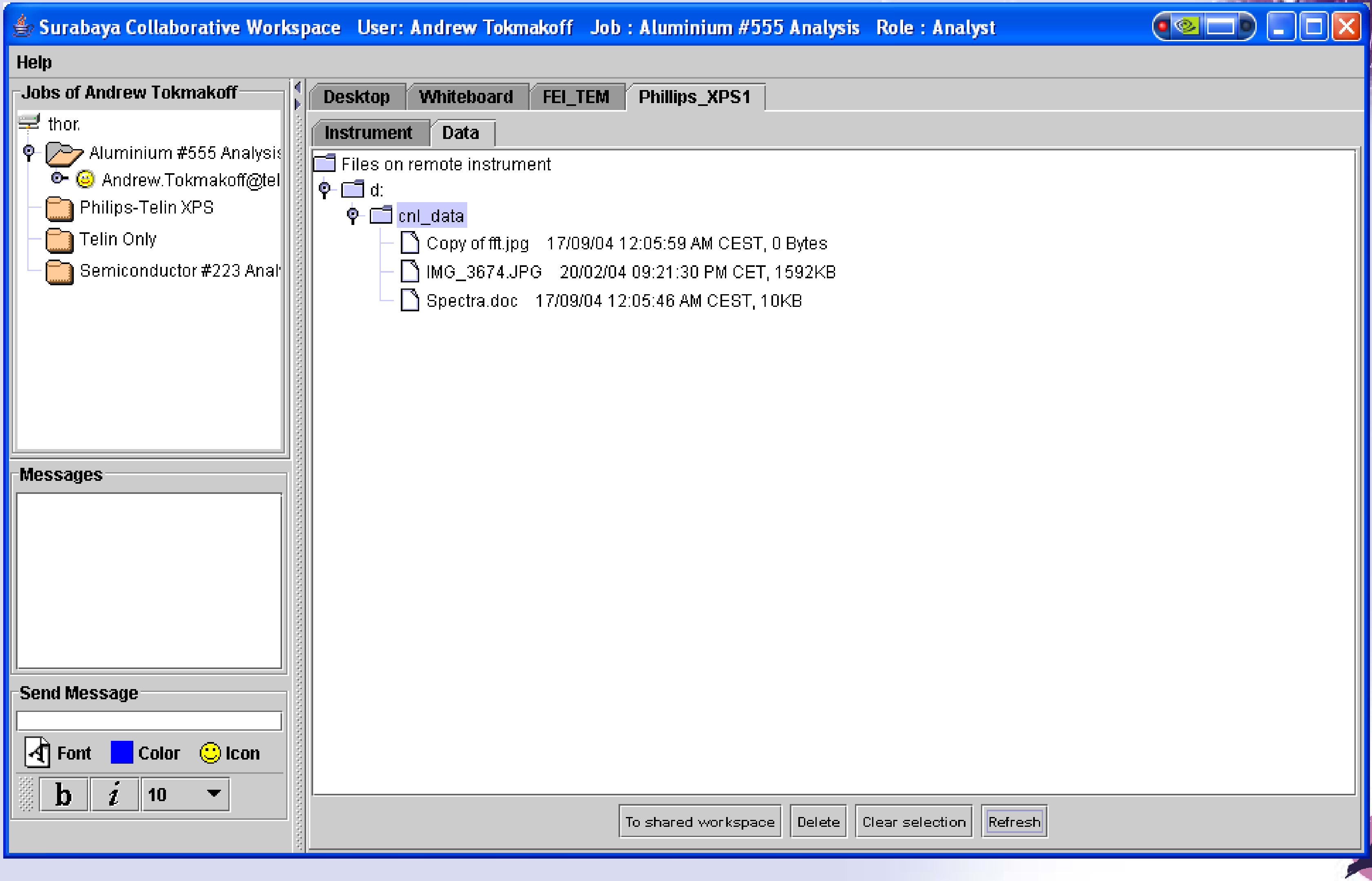
Stage Position: 1/1 File: 4045_19

Acquired/Remaining (min): 2.91/36.62 Region: Al2p

WACE, September 23, 2004

Telematica Instituut

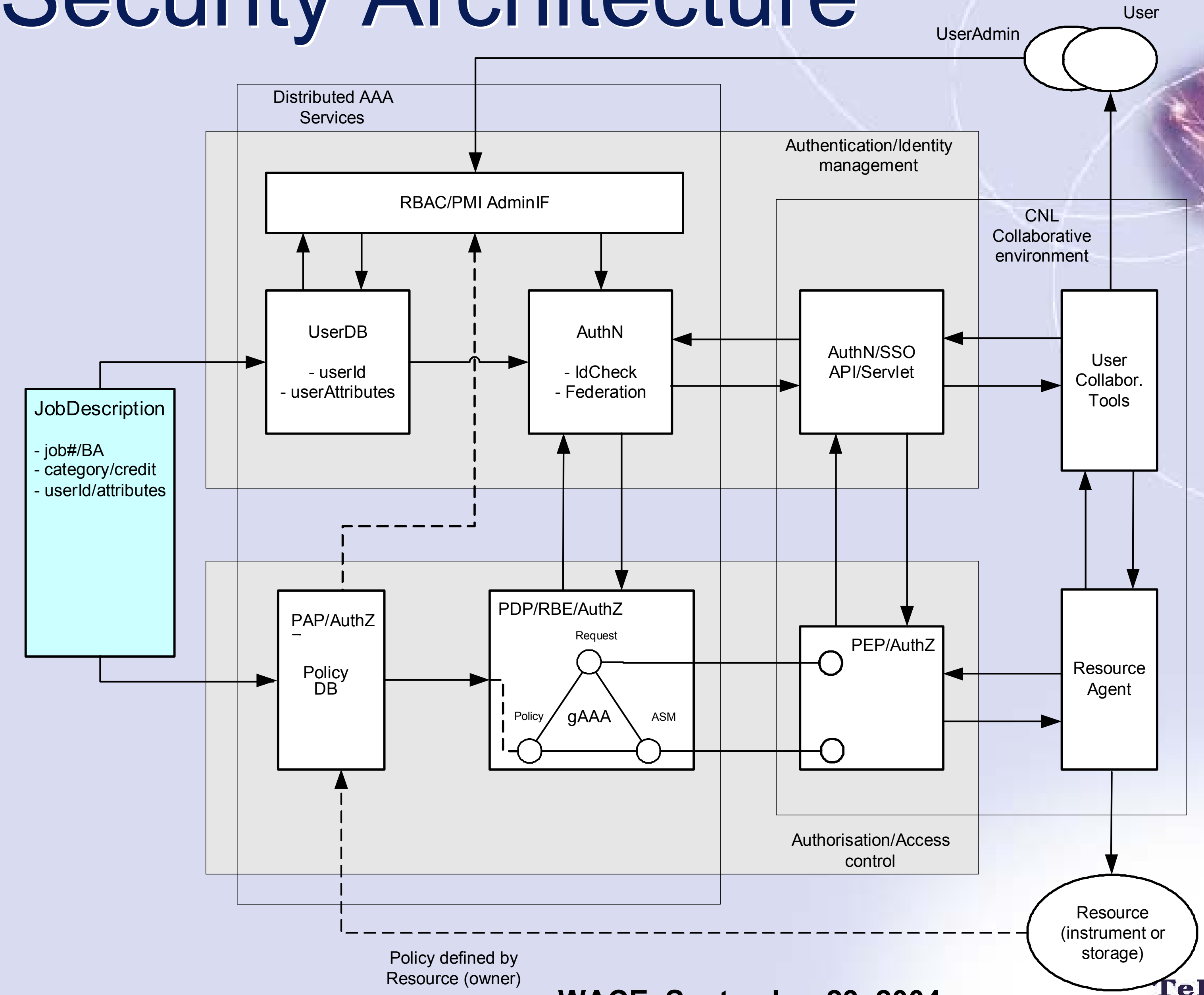
Accessing Remote Data



Surabaya Collaborative Workspace User: Andrew Tokmakoff Job : Aluminium #555 Analysis Role : Analyst

```
Files on remote instrument
d:
  cnl_data
    Copy of fft.jpg    17/09/04 12:05:59 AM CEST, 0 Bytes
    IMG_3674.JPG    20/02/04 09:21:30 PM CET, 1592KB
    Spectra.doc    17/09/04 12:05:46 AM CEST, 10KB
```

Security Architecture



Simplified XACML request

```
<AAA:AAARequest>
  <Subject>
       <SubjectID>UserABC@collaboratory.nl</SubjectID>
       <Role>Analyst</Role>
       <JobID>12a4d5-e44a2b</JobID>
       <Token>2SeDFGVHYTY83ZXxEdsweOP8Iok</Token>
  </Subject>
  <Resource>
       <ResourceID>
            http://res.collaboratory.nl/XPS-Philips1
       </ResourceID>
  </Resource>
  <Action>
       <ActionID>ControlInstrument</ActionID>
  </Action>
</AAA:AAARequest>
```

Simplified XACML response

```
<AAA:AAAResponse>
  <Result ResourceID=http://res.collaboratory.nl/XPS-Philips1>
      <Decision>Permit</Decision >
      <Status>
            <StatusCode value=“OK”/>
            <StatusMessage>
                  Request Succeeded
            </StatusMessage>
      </Status>
  </Result>
</AAA:AAARequest>
```

Summary

- CNL is a “typical” use-case for the OGSA Security Framework.
- CNL’s Security approach:
  - Uses Web Services security technologies and the generic AAA Architecture with a XACML policy-based access control model.
  - allows fine-grained access control and cross-organisation identity management using the VO concept (OGSA).
- Currently in a validation phase.
- Will continue implementing CNL as a VO and adding more business enablers.

Questions?

Offline demo also possible

`Andrew.Tokmakoff@telin.nl`